Pearson Level 3 Alternative Academic Qualification BTEC National in Computing (Extended Certificate)

Unit 2: Computer Network Security and Encryption

Sample Assessment Materials

First teaching September 2025

First certification from 2026

Issue 1

About Pearson

We are the world's leading learning company operating in countries all around the world. We provide content, assessment and digital services to learners, educational institutions, employers, governments and other partners globally. We are committed to helping equip learners with the skills they need to enhance their employability prospects and to succeed in the changing world of work. We believe that wherever learning flourishes so do people.

References to third party materials made in this specification are made in good faith. Pearson does not endorse, approve or accept responsibility for the content of materials, which may be subject to change, or any opinions expressed therein. (Materials may include textbooks, journals, magazines and other publications and websites.)

All information in this document is correct at time of publication.

VQ000352

All the material in this publication is copyright
© Pearson Education Limited 2024

Contents

Unit 1: Question Paper **1**

Unit 1: Mark Scheme **19**

Please check the examination details below before entering your candidate information

Candidate surname	Other names

Centre Number | Learner Registration Number

Pearson Level 3 Alternative Academic Qualification BTEC National in Computing (Extended Certificate)

Sample assessment materials

Time 2 hours 15 minutes

Paper reference XXXXX/XX

Computing

UNIT 2: Computer Network Security and Encryption

You do not need any other materials.

Total Marks

Instructions

- Use **black** ink or ball-point pen.
- **Fill in the boxes** at the top of this page with your name, centre number and learner registration number.
- Answer **all** questions.
- Answer the questions in the spaces provided – *there may be more space than you need.*

Information

- The total mark for this paper is 90.
- The marks for **each** question are shown in brackets – *use this as a guide as to how much time to spend on each question.*

Advice

- Read each question carefully before you start to answer it.
- Try to answer every question.
- Check your answers if you have time at the end.

Turn over ▶

S80453A

©2023 Pearson Education Ltd.

1/1

S 8 0 4 5 3 A 0 1 2 0

Pearson

Answer ALL questions. Write your answers in the spaces provided.

Redpool College is a Further Education establishment that specialises in digital skills and e-learning qualifications.

Melanie is the System Administrator of the Redpool College network.

1 One of Melanie's responsibilities is to ensure that Redpool College's data is stored securely. She uses encryption to help with this.

(a) Melanie could use symmetric or asymmetric encryption.

Symmetric encryption uses a single key for both encryption and decryption.

Asymmetric encryption uses two keys, one to encrypt and the other to decrypt.

(i) Describe **two other** differences between symmetric and asymmetric encryption.

(4)

Difference 1

Difference 2

DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA

(ii) Melanie decides to use an Advanced Encryption Standard (AES) algorithm to protect the data.

AES can have key lengths of 256, 192 or 128 bits. A 256 bit key is more secure than a 192 bit or 128 bit key.

Describe **one** situation where a 128 bit or 192 bit key would need to be used.

(2)

(iii) Using AES-256 implies having a 32 byte password. Most passwords are not 32 bytes long.

Explain how a 256 bit key is produced from a shorter password.

(2)

DO NOT WRITE IN THIS AREA
DO NOT WRITE IN THIS AREA
DO NOT WRITE IN THIS AREA

(b) Redpool College has 600 students who take classes at the campus and another 1500 who are enrolled for distance learning.

Melanie must ensure communications security for the 1500 distance learning students.

One aspect of student communications is email. This uses Simple Mail Transfer Protocol (SMTP).

(i) Give **one other** protocol that is used by email.

(1)

(ii) Describe the role of SMTP in transmitting an email.

(2)

(iii) SMTP is said to be inherently insecure.

Explain the effect that this has on the college's email.

(2)

DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA

(c) Melanie must ensure that Redpool College's data is stored securely. The data is kept in a separate file server and is encrypted using the AES-256 algorithm.

The file server is also protected by a hardware firewall between it and the rest of the network.

Evaluate the effectiveness of this strategy in storing data securely and how it might be improved.

Your evaluation should include the benefits and drawbacks of the strategy, and a conclusion about how Redpool College could improve it.

(9)

(Total for Question 1 = 22 marks)

DO NOT WRITE IN THIS AREA
DO NOT WRITE IN THIS AREA
DO NOT WRITE IN THIS AREA

2 Redpool College has 600 students who take classes at the Redpool College campus and another 1500 who are enrolled for distance learning.

Each student is given 25 Gb of personal storage when they join Redpool College.

Each student is also given access to a storage area to use when working on assignments. The size of these areas can vary from a minimum of 1 Gb, up to 100 Gb, depending on the type of assignment.

Melanie, the System Administrator, must ensure that there is enough data storage available and that the data is kept safe.

(a) The students' personal storage area is kept on a data server at Redpool College.

(i) Explain **one** security-related **advantage** for Redpool College in doing this.

(2)

(ii) Explain **one** security-related **disadvantage** for Redpool College in doing this.

(2)

DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA

(iii) Give **two** ways by which the personal storage can be protected from loss due to failure of the data server.

(2)

(b) The assignment storage areas are kept on cloud storage. Data moving to and from the storage is kept secure by using a Virtual Private Network (VPN).

(i) Describe how a VPN secures moving data.

(3)

(ii) Explain **one** disadvantage of using a VPN in this context.

(2)

DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA

(iii) Describe how a student can check that their VPN client is working.

(3)

DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA

(c) Evaluate the implications of using cloud storage instead of a data server for Redpool College's assignment storage needs.

Your evaluation should include the benefits and drawbacks of each, and a conclusion about which Redpool College should use.

(9)

(Total for Question 2 = 23 marks)

DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA

3 Redpool College has its own Local Area Network (LAN).

The network is run from the IT Centre in the Administration building.

All internet access is routed through a high speed link in the IT Centre.

Melanie uses a range of tools and techniques to help her administer the system.

(a) Penetration testing tools help Melanie identify weaknesses in the system. She uses a network mapping tool to create an inventory of all the devices on the network.

The tool displays IP addresses and other information.

(i) State **two other** pieces of information that a network mapping tool would display.

(2)

.....

.....

.....

.....

(ii) Explain **one** disadvantage of using a network mapping tool for this purpose.

(2)

.....

.....

.....

.....

DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA

(b) Melanie has installed a network intrusion detection system (IDS) and a network intrusion prevention system (IPS).

(i) Describe how an **IPS** differs from an **IDS**.

(2)

(ii) Describe how an **IDS** works.

(3)

DO NOT WRITE IN THIS AREA
DO NOT WRITE IN THIS AREA
DO NOT WRITE IN THIS AREA

(c) Melanie uses a network protocol analysis tool, commonly known as a packet sniffer, to analyse traffic flow within the network.

The tool enables her to find congested routes or bottlenecks in the LAN.

Describe how the tool works in enabling her to find a bottleneck.

(4)

DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA

(d) Melanie must produce risk assessments for the Redpool College LAN. She uses a range of tools and techniques to identify vulnerabilities.

Evaluate the importance of risk assessment and vulnerability scanning in maintaining the security of the LAN.

Your evaluation should explain the benefits of each, and include a conclusion about how Redpool College could make effective use of them.

(9)

(Total for Question 3 = 22 marks)

DO NOT WRITE IN THIS AREA
DO NOT WRITE IN THIS AREA
DO NOT WRITE IN THIS AREA

4 Redpool College has its own Local Area Network (LAN) that is controlled from the IT Centre.

The college employs several technical staff, including some trainees.

Melanie needs to produce training materials for the trainees. This includes information about encryption methods and uses.

(a) Melanie wants to train them on Transport Layer Security (TLS).

(i) Describe what **Transport Layer** refers to in the Redpool LAN.

(2)

(ii) When a client and server connect using TLS they perform a handshake. Describe the role of encryption in performing the handshake.

(2)

(iii) Describe the relationship between TLS and HTTPS.

(2)

DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA

DO NOT WRITE IN THIS AREA

(b) Melanie wants to train them on digital signatures and digital certificates.

(i) Describe the difference between a digital signature and a digital certificate.

(2)

(ii) Describe the role of encryption in **creating** a digital signature.

(3)

DO NOT WRITE IN THIS AREA
DO NOT WRITE IN THIS AREA
DO NOT WRITE IN THIS AREA

(c) Melanie knows that modern cryptographic cyphers are often derived from older, pre-computer methods.

(i) The one-time-pad is a pre-computer cryptographic method that is impossible to break if used correctly. It is now important in the realm of quantum computing.

Give **three** requirements for using a one-time-pad.

(3)

.....

.....

.....

.....

.....

DO NOT WRITE IN THIS AREA
DO NOT WRITE IN THIS AREA
DO NOT WRITE IN THIS AREA

(ii) The substitution cypher has been developed into modern block cyphers.

The Caesar Cypher is an example of a pre-computer substitution cypher. It applies a key (shift value) to a plaintext message and returns an encrypted text. The message consists of single case letters, with no spaces, numbers or other characters.

Develop a simple algorithm for a Caesar Cypher encryption method.

The algorithm should be given in the form of a set of statements in English.

Do **not** submit anything written in a scripting or programming language.

(9)

(Total for Question 4 = 23 marks)

TOTAL FOR PAPER = 90 MARKS

DO NOT WRITE IN THIS AREA
DO NOT WRITE IN THIS AREA
DO NOT WRITE IN THIS AREA

Unit 2: Computer Network Security and Encryption

General marking guidance

- All students must receive the same treatment. Examiners must mark the first student in exactly the same way as they mark the last.
- Mark grids should be applied positively. Students must be rewarded for what they have shown they can do rather than be penalised for omissions.
- Examiners should mark according to the mark grid, not according to their perception of where the grade boundaries may lie.
- All marks on the mark grid should be used appropriately.
- All the marks on the mark grid are designed to be awarded. Examiners should always award full marks if deserved. Examiners should also be prepared to award zero marks, if the student's response is not rewardable according to the mark grid.
- Where judgement is required, a mark grid will provide the principles by which marks will be awarded.
- When examiners are in doubt regarding the application of the mark grid to a student's response, a senior examiner should be consulted.

Specific marking guidance

The mark grids have been designed to assess students' work holistically.

Rows in the grids identify the assessment focus/outcome being targeted. When using a mark grid, the 'best fit' approach should be used.

- Examiners should first make a holistic judgement on which band most closely matches the student's response and place it within that band. Students will be placed in the band that best describes their answer.
- The mark awarded within the band will be decided based on the quality of the answer in response to the assessment focus/outcome and will be modified according to how securely all bullet points are displayed at that band.

- Marks will be awarded towards the top or bottom of that band depending on how they have evidenced each of the descriptor bullet points.

Question Number	Answer	Mark
1 ai	For Difference 1 and Difference 2: Award one mark for each characteristic and one mark for an appropriate linked description of the difference up to a maximum of two marks. • Cipher text (1) is larger in asymmetric (than symmetric) (1) • Encryption (process) (1) is faster for symmetric (than asymmetric) (1) • Key length/size (1) is smaller in symmetric (than asymmetric)/is 128 or 256 for symmetric and 2048 for asymmetric (1) • Resources used/needed (1) are lower for symmetric (than asymmetric) (1) • efficiency (1) is greater for symmetric (than asymmetric) (1) • security (1) is greater for symmetric (than asymmetric) (1) • authenticity/non-repudiation (1) is greater for asymmetric/does not exist in symmetric (1) Do not accept answers about number/type of keys needed. Accept reverse arguments, such as Cipher text is smaller for symmetric (than asymmetric). Do not award both versions of an answer.	**(4)**

2

Question Number	Answer	Mark
1 aii	Award one mark for each appropriate point in a linked description up to a maximum of two marks. • Connection/internet/network speed/data transmission rate is low/limited (1) and needs a reduced data load (1) • Mobile/battery powered device is being used (1) and has less power/processing (1) Accept any other appropriate responses. Do not accept answers about security levels.	**(2)**

Question Number	Answer	Mark
1 aiii	Award one mark for identification of a process and one mark for an appropriate linked expansion, up to a maximum of two marks. Use of a hashing algorithm/function (1) to expand a short key (1) Expand a short key (1) by repeating the algorithm/function until key length is long enough/256 bits (1) Repeat a hashing algorithm/function (1) until the key length is long enough/256 bits (1) Accept any other appropriate responses.	**(2)**

Question Number	Answer	Mark
1 bi	Award one mark for any of the following: • Internet Message Access (Protocol) (1) • Post Office (Protocol) (1) • Post Office Protocol 3 (1) Accept abbreviations: IMAP, POP, POP3.	**(1)**

Question Number	Answer	Mark
1bii	Award one mark for each appropriate point in a linked description up to a maximum of two marks. • Relays/accepts/routes message from originator/user/sender (1) • Handshakes with/connects to receiver/recipient (1) • Releases/delivers email to receiver (1)	**(2)**

Question Number	Answer	Mark
1 biii	Award one mark for identification of a reason and one mark for an appropriate linked expansion, up to a maximum of two marks. • Because the protocol has no security features (1) it makes the email vulnerable to attack/interception (1) • Because of the lack of security (1) (sensitive) emails would need to be encrypted (1)	**(2)**

Question number	Indicative content
1 c	**Award up to 9 marks.** Responses should be in the context of securing Redpool College's data on a file server. Responses will be credited according to the student's demonstration of knowledge and understanding of the material, using the indicative content and level descriptors below. The indicative content that follows is not prescriptive. Responses may cover some or all indicative content, but students should be rewarded for other relevant responses. **Encryption:** • Encryption of data at rest, does not say what happens during data movement • Does not say if individual file or whole disc encryption is used • Encryption ensures that even if data is looked at by unauthorised person, it remains unreadable without the appropriate decryption key. • It protects the confidentiality and integrity of the data, minimising the impact of breaches. • Weak point is password/authentication method, this is not given. **Firewall:** • First line of defence by monitoring incoming and outgoing network traffic • Blocking or allowing data packets based on predefined security rules. • Help to protect the network from unauthorised access and

	malicious traffic. • Hardware firewall usually more effective than software • Weak point is configuring the rules • Network should also have a firewall on its internet connection • Network could have other hardware/software firewalls operating • Having two/multiple firewalls on a network should increase security but could cause problems/clashes • Maintenance/update/patching issues **Conclusion/improvements (this is not a list of marking points - anything sensible and relevant should be accepted):** • Ensure AES_256 or equivalent on moving data • Specify type of encryption, link to authorisation levels • Impose strong password policy/MFA • Check process/testing of firewall rules • Consider how firewalls are deployed to reduce/remove clashes • Ensure all firewalls are maintained/updated/patched to same level

Mark scheme (award up to 9 marks) refer to guidance for how to apply levels-based mark schemes*.		
Level	**Mark**	**Descriptor**
Level 0	0	No rewardable material.
Level 1	1–3	• Demonstrates basic application of knowledge and understanding that is partially relevant to the context of the question (AO2) • Demonstrates a basic analysis by superficially breaking down the different aspects into component parts with errors/inconsistency (AO3) • Demonstrates a basic evaluation which partially considers different factors and competing points, leading to an unsupported conclusion (AO4).
Level 2	4-6	• Demonstrates good application of knowledge and understanding that is relevant to the context of the question (AO2) • Demonstrates a good analysis by breaking down the different aspects into component parts (AO3) • Demonstrates a good evaluation which considers different factors and competing points, leading to a partially

		supported conclusion (AO4).
Level 3	7-9	• Demonstrates comprehensive application of knowledge and understanding that is consistently relevant to the context of the question (AO2) • Demonstrates a thorough analysis by comprehensively breaking down the different aspects into their component parts (AO3) • Demonstrates a thorough evaluation which comprehensively considers different factors and competing points, leading to a well-supported conclusion (AO4).

Question Number	Answer	Mark
2 ai	Award one mark for correct identification of the first point and one mark for an appropriate linked justification, up to a maximum of two marks. • Server is under (direct) control of Redpool College (1) • So easier to ◦ enforce password strength/authorisation/MFA (1) ◦ protect from physical theft/unauthorised physical connection (1) ◦ protect from unauthorised access/hacking (1) Do not accept answers that are not related to security.	**(2)**

Question Number	Answer	Mark
2 aii	Award one mark for identification of a security-related disadvantage and one mark for an appropriate linked justification, up to a maximum of two marks. • Could be a known/attractive target for attacking (1) as large amount of data/number of student accounts (1) • Mistakes could expose (large amounts of) data/accounts (1) as large number of accounts/passwords/authorisations to process/deal with (1) Accept any other appropriate responses. Do not accept answers that are not related to security.	**(2)**

Question Number	Answer	Mark
2 aiii	Award one mark for each way up to a maximum of two marks. • Backup data to separate device(s) (1) • Use RAID_N: N=any version except RAID_0 (1) • Maintenance of storage devices (1) • Replace devices/discs/SSDs early/before end of rated lifetime (1)	**(2)**

Question Number	Answer	Mark
2 bi	Award one mark for each appropriate point in a linked description up to a maximum of three marks. • Routes/forwards data to VPN server (instead of ISP) • VPN (software) encrypts data client side/before sending • VPN (software) creates VPN tunnel/uses tunnelling protocol Accept any other appropriate responses. Do not accept answers not related to security.	**(3)**

Question Number	Answer	Mark
2 bii	Award one mark for a disadvantage and one mark for an appropriate linked expansion, up to a maximum of two marks. • VPN requires more resources/ processing/routing steps (1) which may slow down the internet link/data transfer/system (1) • VPN requires configuration (1) errors may reveal data/reduce security/stop the system working properly (1) • Some countries/states/governments restrict/ban VPNs (1) this may cause legal problems for Redpool College/students (in those places) (1)	**(2)**

Question Number	Answer	Mark
2 biii	Award one mark for each appropriate point in a linked description up to a maximum of three marks. • Find public IP address using third party website/router admin pages/command such as ipconfig (1) • With VPN off, check public IP address (1) • With VPN on, check public IP address (1) • Compare IP addresses, should be different (1) Accept any other appropriate responses.	**(3)**

Question number	Indicative content
2 c	**Award up to 9 marks.** Responses should be in the context of using cloud storage instead of a data server. Responses will be credited according to the student's demonstration of knowledge and understanding of the material, using the indicative content and level descriptors below. The indicative content that follows is not prescriptive. Responses may cover some or all indicative content, but students should be rewarded for other relevant responses. **Benefits:** Cost savings: Cloud-based networks often provide cost savings compared to maintaining on-premises infrastructure. Benefit from economies of scale and pay only for the resources they use. Assignment space needs will vary. Scalability: Cloud networks offer on-demand scalability without significant upfront investments in hardware or software. Data server would need to have enough storage for maximum needs, plus contingency. Flexibility: Cloud networks enable students to access applications and data from anywhere with an internet connection, promoting remote work and collaboration. Better for distance learning students and saves on Redpool College resources. Automatic updates: Cloud service providers typically handle software updates and security patches, ensuring the systems remain up-to-date and secure. Saving maintenance time at the College. **Drawbacks:** Dependency on Internet connectivity: Cloud-based storage relies on stable Internet connections for access and performance. They are vulnerable to connectivity issues and potential downtime. A data server has similar issues but Redpool College will have more control/will know what is happening. Data privacy and security concerns: Storing sensitive data in the cloud may raise concerns about data privacy. The service provider must be trusted to maintain security and

	comply with relevant regulations. Potential vendor lock-in: Migrating from one cloud service provider to another can be challenging/expensive. Technology issues may make it difficult to switch vendors. Overall evaluation: The decision to use a cloud-based network depends on the organisation's specific needs and requirements and the potential risks and benefits. Cost, scalability, and flexibility must be weighed against data privacy, security, and vendor concerns. **Conclusions (this is not a list of marking points – anything sensible and relevant should be accepted, but overall, cloud storage is likely to be the best choice). Look for arguments such as:** • Cost/scalability/flexibility weighed against data privacy/ security/vendor problems. • Cost/scalability/flexibility of data server weighed against cloud storage. • Accessibility by students, especially distance students. • Assignments probably don't involve personal data so may need less security. • Assignments may need more collaboration.

Mark scheme (award up to 9 marks) refer to guidance for how to apply levels-based mark schemes*.		
Level	**Mark**	**Descriptor**
Level 0	0	No rewardable material.
Level 1	1–3	• Demonstrates basic application of knowledge and understanding that is partially relevant to the context of the question (AO2) • Demonstrates a basic analysis by superficially breaking down the different aspects into component parts with errors/inconsistency (AO3) • Demonstrates a basic evaluation which partially considers different factors and competing points, leading to an unsupported conclusion (AO4).
Level 2	4–6	• Demonstrates good application of knowledge and understanding that is relevant to the context of the question (AO2) • Demonstrates a good analysis by breaking down the different aspects into component parts (AO3) • Demonstrates a good evaluation which considers different factors and competing points, leading to a partially supported conclusion (AO4).
Level 3	7–9	• Demonstrates comprehensive application of knowledge and understanding that is consistently relevant to the context of the question (AO2) • Demonstrates a thorough analysis by comprehensively breaking down the different aspects into their component parts (AO3) • Demonstrates a thorough evaluation which comprehensively considers different factors and competing points, leading to a well-supported conclusion (AO4).

Question Number	Answer	Mark
3 ai	Award one mark for each appropriate point up to a maximum of two marks. • Host/device names (1) • Running services (1) • OS details, version/patch numbers (1) • Ports open/used (1) • Network topology (map) (1) Do not accept answers about IP addresses.	**(2)**

Question Number	Answer	Mark
3 aii	Award one mark for identification of a disadvantage and one mark for an appropriate linked justification, up to a maximum of two marks. • Tool generates a lot of traffic/noise (1) which can trigger IDS/IPS (1) • Tool can only detect working/running systems/hosts/services (1) so giving an incomplete picture (of the network) (1) • Tool can generate false positives/incorrect data (1) so giving an incorrect picture (of the network) (1) Accept any other appropriate responses.	**(2)**

Question Number	Answer	Mark
3 bi	Award one mark for each appropriate point in a linked description up to a maximum of two marks. IPS takes action to stop (suspicious) activity (1) IDS only produces a log/alert (1)	**(2)**

Question Number	Answer	Mark
3 bii	Award one mark for each appropriate point in a linked description up to a maximum of three marks. • Monitors network traffic (1) • Detects intrusion based on signature/anomalies/heuristics/policy violations/malicious activity (1) • Generates log (1) • Alerts user (1) Accept any other appropriate responses.	**(3)**

Question Number	Answer	Mark
3 c	Award one mark for each appropriate point in a linked description up to a maximum of four marks. • Intercepts data packets (1) • Only intercepts small percentage/proportion/sample of packets (1) • Stores/logs packet header/control information (1) • Analyses packet header/control information (1) • Presents data in user-readable form/as chart/table/other suitable form (1) • Shows devices/nodes/locations with unusual packet loss/repeat requests/failure to respond (1) Accept any other appropriate responses.	**(4)**

Question number	Indicative content
3 d	**Award up to 9 marks.** Responses should be in the context of risk assessment and vulnerability scanning for Redpool College's LAN. Responses will be credited according to the student's demonstration of knowledge and understanding of the material, using the indicative content and level descriptors below. The indicative content that follows is not prescriptive. Responses may cover some or all indicative content, but students should be rewarded for other relevant responses. **Identifying potential risks and vulnerabilities:** Vulnerability scanning helps identify possible threats and weaknesses in the network. Risk assessments are a formal way of setting out/categorising/prioritising the risks. Both enable the college to address the issues proactively. Both help identify possible risk reduction measures. **Prioritising resources:** Help understand the risks and vulnerabilities, so resources can be focussed on the most critical areas. Identifies areas where new software/devices/technology can help reduce risks. **Compliance with regulations:** Regular risk assessments and vulnerability scanning help ensure compliance with data protection laws and regulations. **Improving ongoing/future security**: Carrying out risk assessments and vulnerability scans helps continuously improve security measures. Adapting to evolving threats. Maintaining a robust security approach. Helps keep up with latest ideas/knowledge/security measures. **Reducing the impact of breaches:** Identifying and addressing vulnerabilities can help minimise potential breaches' impact, reducing costs and reputational damage. **Conclusions (this is not a list of marking points – anything sensible and relevant should be accepted):** • Regular updates of risk assessments. • Based on results of vulnerability scans.

	• Based on changes in the threat landscape. • Ensure latest patches/updates applied to scanning tools, so keeping up with changes/developments in threats.

Mark scheme (award up to 9 marks) refer to guidance for how to apply levels-based mark schemes*.		
Level	**Mark**	**Descriptor**
Level 0	0	No rewardable material.
Level 1	1–3	• Demonstrates basic application of knowledge and understanding that is partially relevant to the context of the question (AO2) • Demonstrates a basic analysis by superficially breaking down the different aspects into component parts with errors/inconsistency (AO3) • Demonstrates a basic evaluation which partially considers different factors and competing points, leading to an unsupported conclusion (AO4).
Level 2	4-6	• Demonstrates good application of knowledge and understanding that is relevant to the context of the question (AO2) • Demonstrates a good analysis by breaking down the different aspects into component parts (AO3) • Demonstrates a good evaluation which considers different factors and competing points, leading to a partially supported conclusion (AO4).
Level 3	7-9	• Demonstrates comprehensive application of knowledge and understanding that is consistently relevant to the context of the question (AO2) • Demonstrates a thorough analysis by comprehensively breaking down the different aspects into their component parts (AO3) • Demonstrates a thorough evaluation which comprehensively considers different factors and competing points, leading to a well-supported conclusion (AO4).

Question Number	Answer	Mark
4 ai	Award one mark for each appropriate point in a linked description up to a maximum of two marks. • Part of OSI/TCPIP stack/protocol/model (1) (layer) handles host-host/source-receiver data transfer (1)	**(2)**

Question Number	Answer	Mark
4 aii	Award one mark for each appropriate point in a linked description up to a maximum of two marks. EITHER • Session keys generated (1) using a random number/ server public key (1) OR • Session keys generated (1) using (Diffie–Hellman) key exchange (1)	**(2)**

Question Number	Answer	Mark
4 aiii	Award one mark for each of the following points, up to a maximum of two marks. • HTTPS piggybacks HTTP over TLS (1) • This creates a secure channel (1) • This allows the encryption of the HTTP traffic (1) Accept any other appropriate responses.	**(2)**

Question Number	Answer	Mark
4 bi	Award one mark for each appropriate point in a linked description up to a maximum of two marks. • Digital signature verifies data is secure/can be trusted/is as sent (1) digital certificate verifies sender is who they say they are/can be trusted (1)	**(2)**

Question Number	Answer	Mark
4 bii	Award one mark for each appropriate point in a linked description up to a maximum of three marks. • Hash created of message/data (1) • Hash is one-way (1) • Hash (value) encrypted with (private) key (1) • Encrypted hash is the digital signature (1) Do not accept answers that are about processes other than encryption, e.g. sending/receiving messages. Do not accept answers about processes after signature creation, e.g. decrypting signature.	**(3)**

Question Number	Answer	Mark
4 ci	Award one mark for each appropriate point up to a maximum of three marks. • Key/pad must not be reused/must only be used once (1) • Key/pad must be kept secret (1) • Key/pad must be larger/at least as large as the plaintext/message (1) • Key/pad must be random (1)	**(3)**

Question Number	Answer	Mark
4 cii	Award one mark for each appropriate point up to a maximum of nine marks. 1. Input message (1) 2. Input key/value shift (1) 3. Find/identify first letter (1) 4. Identify letter number/find position in alphabet (1) 5. Add/count forward key/value shift (1) 6. If count goes past Z, resume at A (1) 7. Record cyphertext letter (1) 8. Remove/move one on from current letter (1) 9. If no more letters in message then stop (1) 10. Otherwise go back to instruction 4 (1) (this could be an arrow/line) Do not accept statements that are obviously in a scripting or programming language.	**(9)**

July 2024

For information about Pearson Qualifications, including Pearson Edexcel and BTEC qualifications visit qualifications.pearson.com

Edexcel and BTEC are registered trademarks of Pearson Education Limited

Pearson Education Limited. Registered in England and Wales No. 872828
Registered Office: 80 Strand, London WC2R 0RL.

VAT Reg No GB 278 537121